SPECIFICATION AMENDMENTS

Please replace paragraph [0030] of the published version of the specification with the following rewritten paragraph:

In ~~a~~ another embodiment, the DRM user unit further comprises a revocation list storage unit for storing a revocation list of DRM client units, said revocation list being checked by said authentication unit during authentication of a DRM client unit. Thus, the DRM user unit can check during authentication of a DRM client unit if the DRM client is a valid client or not, and can restrict the access of particular DROs or all DROs stored on the DRM client, if the DRM client is listed in the revocation list.

Please replace paragraph [0031] of the published version of the specification with the following rewritten paragraph:

The data and algorithms in the DRM user unit can be updated during a connection between the DRM user unit and the DRM server of the service provider. This update procedure is preferably protected by cryptographic keys to ensure that only ~~authorised~~ authorized instances are able to carry out changes of the data and algorithms of the DRM user unit. If the DRM user unit is represented by a smart card or uses a smart card IC as an authentication unit, the additional smart card security measures ensure that no illicit access to the DRM user unit can be made.

Please replace paragraph [0044] of the published version of the specification with the following rewritten paragraph:

The currently known systems for ~~a digital rights management~~ DRM feature three main functional entities: a DRM client in a DRM client unit at the customer side, a DRM server at a service provider[[,]] which issues the DROs, and a content provider that issues the DDOs. The disadvantage of this system from the user perspective is that the DRO issued by the DRM server can be used only by one particular DRM client, and ~~in the presently known systems~~ that the DRM client is assigned to one particular electronic device or to a group of electronic devices that are functionally dependent on each other. In other words, it is an intrinsic feature of the presently known DRM systems, that the DRO that a customer purchases ~~can not~~ cannot be used like a personal license to use the related content on ~~the~~ playback devices of choice. Hence, the content can only be played back on a fixed device, regardless who ~~possess~~ possesses this device. The reason for this is to guarantee that each DRO represents exactly one permission to use the DDO. This guarantees that no "copies" in any form can be made of the purchased content. To assure this, a DRM client is authenticated before[[,]] a DRO is issued to the DRM client. The authentication of the DRM client includes ~~the~~ checking a revocation list that has registered devices that are reported broken or possibly broken. Based on the authentication data of the DRM client and possible entries in the revocation list,

a DRO is issued to the DRM client or the issuing of the DRO to the DRM client is denied.

Please replace paragraph [0049] of the published version of the specification with the following rewritten paragraph:

The operation of the DRM system can be seen from FIGS. 2 and 3. In FIG. 2, the transfer of a DRO from the DRM ~~sever~~ server unit 1 to the DRM user unit 2 is shown. In order for the DRM user unit 2 to obtain a DRO and for the DRM server unit 1 to possibly update the authentication algorithm and the revocation list, a mutual authentication between the DRM user unit 2 and the DRM server unit 1 has to ~~be traded out~~ occur. ~~Especially the~~ The DRM server unit 1 checks if the DRM user unit 2 is recorded in the revocation list stored in the revocation list storage 12. After a successful authentication, several actions are possible, such as grant of a digital rights object, update of an authentication algorithm, or update of the revocation list stored in the revocation list storage 22 of the DRM user unit 2.

Please replace paragraph [0058] of the published version of the specification with the following rewritten paragraph:

The DRM user unit can be represented by a smart card. In this case, the DRM user unit does not have ~~an~~ its own user interface, so for any operation that

requires ~~a~~ user interaction, the smart card has to be linked to a device that can handle the user I/O. Primarily, there are three different devices that will be used as I/O devices for a smart card that functions as the DRM user unit:

Please replace paragraph [0064] of the published version of the specification with the following rewritten paragraph:

The following usage scenarios outline the possible use of a DRM user unit mostly on the ~~base~~ basis of an NFC enabled mobile terminal. The handling of the DRO can be implemented on smart cards as well, but the use of an NFC device brings additional functionality to the system.

Please replace paragraph [0066] of the published version of the specification with the following rewritten paragraph:

In a further usage scenario, the consumer watches a broadcast of an ~~impressing~~ impressive concert at home. At the end of the performance, the broadcaster shows an advertisement[[,]] stating that for a very special price a non-transferable limited DRO of the performance with 5 presentation times can be purchased online. The consumer wants to take advantage of this special offer and connects his stereo system via the NFC interface and GSM connection of his mobile phone to the DRM server of the provider. The DRM server authenticates both[[,]]

the DRM user unit (mobile terminal) as well as the DRM client (stereo set). After the successful authentication and a payment via the VISA applet of the mobile phone, the DRO for the concert is transferred to the mobile phone. This particular DRO can be used only in conjunction with the specific stereo set (non-transferable DRO).